Hacia el Pearl Harbor cibernético

El Gobierno de EE UU confiesa su preocupación por la escalada de la ciberguerra con Irán, que ha atacado sistemas informáticos estadounidenses en respuesta a las agresiones virales sufridas

Por JAVIER VALENZUELA

Tan silenciosa es esta guerra, que la inmensa mayoría del planeta ni se ha enterado de que se libra con ferocidad desde hace tiempo. Los que están en ella la viven, sin embargo, con creciente angustia. Por ejemplo, Leon Panetta, que acaba de declarar que su país está al borde de "un Pearl Harbor cibernético". ¿A qué se refiere el secretario de Defensa de Estados Unidos? Pues a una reciente serie de ataques contra sistemas informáticos de la industria petrolera saudí e instituciones financieras norteamericanas atribuidos, según informó *International Herald Tribune* en su edición del lunes pasado, a las unidades de defensa contra la ciberguerra puestas en pie por la República Islámica de Irán.

¿Guerreros ciberespaciales del régimen de los ayatolás? Sí, existen desde 2011 como respuesta a una previa ofensiva de piratería informática de su programa nuclear universalmente atribuida a la colaboración de Estados Unidos e Israel. En principio, su tarea consistía en hacer ducido la presencia de tropas físicas estadounidenses en zonas conflictivas.

En la noche del martes al miércoles, en su segundo debate televisado de esta campaña presidencial, Obama le paró los pies a Romney a propósito de una supuesta "blandura" en el caso del asalto al consulado norteamericano en Bengasi. Tenía razón: no es para nada la "paloma" que describen esos belicosos a la antigua que son los republicanos de Estados Unidos; es un frío, inteligente e implacable comandante en jefe de las nuevas formas de hacer la guerra en el siglo XXI.

La ciberguerra contra Irán comenzó durante la presidencia del segundo Bush y en ella van cogidos de la mano Estados Unidos e Israel. Su primer producto conocido, el virus Stuxnet, perturbó seriamente las instalaciones nucleares iraníes a finales de la pasada década. Al ser descubierto en el verano de 2010 —se fugó a Internet desde la planta iraní de Natanz—, Obama hizo patente su preocupación en las reuniones de su consejo de seguridad en la Casa Blanca. Dijo temer que la conversión de Estados Unidos en un musculoso *hacker* con bandera nacional terminara justificando política y mofirmar sus propias debilidades, el régimen iraní terminaría reconociendo que troyanos, virus y programas malignos venidos del exterior zancadilleaban sus esfuerzos.

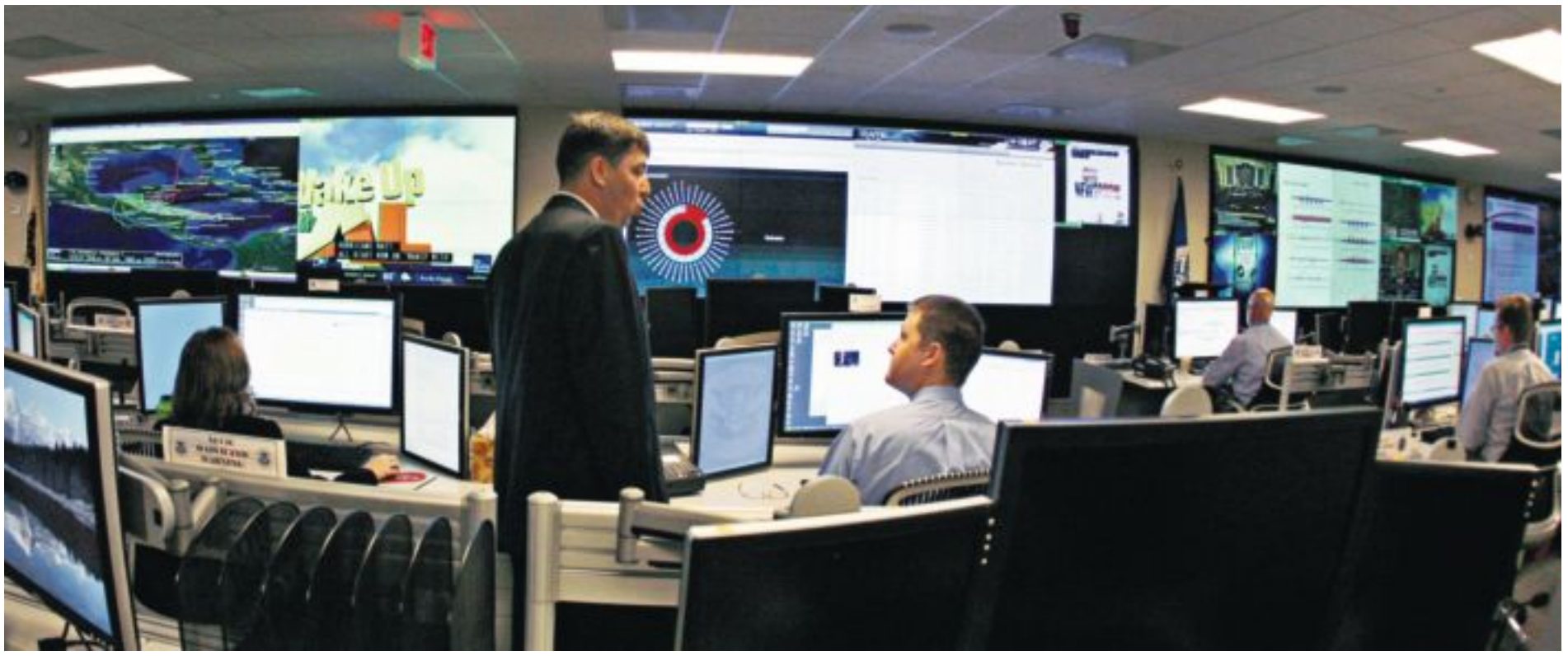
En 2010, Richard A. Clarke, que fue jefe de los servicios antiterroristas de Estados Unidos con Bill Clinton y George W. Bush, publicó un ensayo titulado *Cyber War* (publicado en castellano por Ariel con el título *Guerra en la red).* Profetizaba una III Guerra Mundial en el ciberespacio para la que ya se estaban preparando potencias como Estados Unidos, Israel, Rusia y China. Así lo reseñó, muy críticamente, la revista *Wired:* "Encontrarán aquí el *Libro de las revelaciones* vuelto a escribir para la era de Internet, con el Fin de los Tiempos anunciado por los Cuatro Caballos Troyanos del Apocalipsis".

¿Es Flame el primero de esos caballos? A finales de mayo, el organismo público iraní dedicado a la lucha contra la piratería informática (CERT en sus siglas en inglés) anunció que había localizado ese virus, el más maligno de los jamás inventados. Llevaba dos años infectando sus ordenadores sin ser detectado por ningún antivirus.

Flame es un conjunto de programas que realiza múltiples tareas de espionaje y sabotaje: graba conversaciones, permite control remoto del ordenador, tiene Bluetooth que se adueña de los teléfonos móviles próximos, copia y transmite datos a distancia, se va actualizando, es indetectable por los antivirus hoy existentes... Según observó Douglas Rushkoff en CNN, "tiene todos los indicios de constituir un ciberataque maquinado por un Estado nación".

Su descubrimiento fue obra del laboratorio especializado que el ruso Eugene Kaspersky dirige en Moscú. Kaspersky lo tildó de "caja de Pandora", aseguró que el uso de virus como este podría terminar afectando a servicios civiles nacionales enteros como redes eléctricas, industrias energéticas, redes bancarias o sistemas de tráfico aéreo, por lo que, añadió, deberían ser prohibidos, como en su día lo fueron las armas químicas y biológicas. "Estoy asustado, créanme", declaró.

Por supuesto, Estados Unidos no reconoce oficialmente ninguna relación con estos virus informáticos que minan el programa nuclear iraní. Tampoco lo hace Israel.



Un departamento de seguridad encargado de evitar que se produzcan ataques a sistemas informáticos estadounidenses en Arlington (Virginia). Foto: Hyungwon Kang / Reuters

de antivirus para proteger los sistemas iraníes, pero, según las fuentes citadas por el *Tribune,* podrían haber pasado a la contraofensiva con los ataques que en agosto afectaron a la compañía petrolera estatal saudí Aramco y tal vez los que impidieron a clientes de bancos norteamericanos acceder *online* a sus cuentas.

Aunque sean de oficio los *villanos* de la película, no fueron los ayatolás los primeros en apretar este botón. Lo hizo un premio Nobel de la Paz, el mismísimo Barack Obama. En su primer mandato presidencial, Obama se ha caracterizado por un modo peculiar —más contemporáneo, por así decirlo, y, para él y sus compatriotas, menos traumático— de hacer la guerra: el desarrollo de la ciberguerra (ciberespionaje y cibersabotaje) contra Irán y el uso masivo de drones —aviones sin humanos a bordo— para atacar objetivos en países como Somalia, Yemen, Afganistán y Pakistán. Por el contrario, ha reralmente ciberataques contra ese mismo país. Es una opinión que hoy siguen expresando otros en Estados Unidos.

Pero las dudas de Obama se desvanecieron pronto y terminó aprobando la continuidad de esa forma de pelea, conocida en la Casa Blanca, el Pentágono y la CIA como *Olimpic Games.* Incluso hizo más: decretó su escalada. A comienzos de julio, *The New York Times* publicó una extensa información que daba cuenta de cómo Obama "ordenó en secreto un aumento de los ataques sofisticados a los sistemas informáticos de las factorías iraníes de enriquecimiento de uranio, expandiendo así de modo significativo el primer uso continuado por Estados Unidos de ciberarmas".

A la par, Obama instó a los servicios de inteligencia civiles y militares norteamericanos a estrechar la colaboración en este frente con los israelíes. Tras negarlo inicialmente, por aquello de no con-

En mayo, Irán anunció que había localizado en sus ordenadores el virus Flame, el más maligno jamás inventado

Según 'The New Yorker', la Fuerza Aérea de EE UU cuenta con 7.000 ciberguerreros en bases de Tejas y Georgia

Eso sí, *The New Yorker* informa de que tan solo la Fuerza Aérea de Estados Unidos cuenta ya con 7.000 ciberguerreros en bases de Tejas y Georgia. ¿Cuántos más habrá en otros departamentos del Pentágono, la CIA y otros órganos del Gobierno federal estadounidense?

Creado en 2009, bajo la presidencia de Obama, con sede oficial en Fort Meade (Maryland) y dirigido por el general Keith B. Alexander, United States Cyber Command (Uscybercom) es el nombre del organismo que dirige las unidades ciberespaciales de la Fuerza Aérea norteamericana. Ahora parece haberle surgido un serio rival en las unidades iraníes especializadas que dirige el general Gholamreza Jalali y que podrían estar detrás de los últimos ataques a sistemas saudíes y estadounidenses. Aún no ha sonado un solo disparo en la próxima guerra del Golfo, pero, a golpe de teclado y de ratón, esta se libra ya en el ciberespacio. •